

**IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF FLORIDA  
WEST PALM BEACH DIVISION**

YVETTE TITTSWORTH on behalf of herself  
and all others similarly situated,

Plaintiff,

v.

HAIRCLUB FOR MEN, LTD., INC.,

Defendant.

NO. 9:24cv80349

**DEMAND FOR JURY TRIAL**

**CLASS ACTION COMPLAINT**

Plaintiff, Yvette Tittsworth (“Plaintiff”), on behalf of herself and all others similarly situated, states as follows for her class action complaint against Defendant, HairClub for Men, Ltd., Inc. (“HairClub” or “Defendant”):

**INTRODUCTION**

1. On October 17, 2023, HairClub lost control over its computer network and the highly sensitive personal information stored on the computer network in a data breach by cybercriminals (“Data Breach”). On information and belief, the Data Breach has impacted 4334 individuals.

2. HairClub was founded in 1976 and is “North America’s number one provider of hair regrowth, replacement, and restoration solutions.” HairClub has more than 120 locations throughout the United States, Canada, and Puerto Rico and proclaims itself as the “world’s leading provider of total hair loss solutions.”<sup>1</sup>

---

<sup>1</sup> *HairClub Celebrates Season of Giving by Helping Seniors in Need*, HairClub, <https://www.hairclub.com/press-release/hairclub-celebrates-season-of-giving-by-helping-seniors-in-need-2/> (last visited March 20, 2024).

3. Due to Defendant's intentionally obfuscating language, it is unclear when the Data Breach precisely occurred and how long cybercriminals had unfettered access to Plaintiff's and the Class's highly sensitive information. However, on information and belief, the breach took place between October 17, 2023 and October 18, 2023.<sup>2</sup> Defendant did not discover the breach until December 1, 2023.

4. Following an internal investigation, Defendant learned cybercriminals gained unauthorized access to employees' personally identifiable information ("PII"), including but not limited to their name, Social Security number, driver's license information, direct deposit account information and medical information related to injuries at work or requests for family or medical leave.

5. On or about January 12, 2024—almost three months after the Data Breach occurred—Defendant finally began notifying Plaintiff and Class Members about the Data Breach ("Breach Notice"). An example of the Breach Notice is attached as Exhibit A.

6. Upon information and belief, cybercriminals were able to breach Defendant's systems because Defendant failed to adequately train its employees on cybersecurity, failed to adequately monitor its agents, contractors, vendors, and suppliers in handling and securing the PII of Plaintiff, and failed to maintain reasonable security safeguards or protocols to protect the Class's PII—rendering them easy targets for cybercriminals.

7. Defendant's Breach Notice obfuscated the nature of the breach and the threat it posed—refusing to tell its employees how many people were impacted, how the breach happened, when the Breach occurred, or why it took the Defendant over three months to begin notifying

---

<sup>2</sup> Data Breach Notifications, Office of the Maine Attorney General, <https://apps.web.maine.gov/online/aeviewer/ME/40/d570ad19-5ac8-4b21-8b2c-1330a5e7c386.shtml> (last visited March 20, 2024).

victims that cybercriminal had gained access to their highly private information.

8. Defendant's failure to timely report the Data Breach made the victims vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

9. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

10. In failing to adequately protect employees' information, adequately notify them about the breach, and obfuscating the nature of the breach, Defendant violated state law and harmed a staggering number of employees.

11. Plaintiff and the Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendant with their PII. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

12. Plaintiff is a former employee of Defendant and is a Data Breach victim.

13. The exposure of one's PII to cybercriminals is a bell that cannot be unrung. Before the Data Breach, the private information of Plaintiff and the Class was exactly that—private. Not anymore. Now, their private information is permanently exposed and insecure.

### **PARTIES**

14. Plaintiff, Yvette Tittsworth, is a natural person and citizen of Florida, residing in Boynton Beach, Florida, where she intends to remain.

15. Defendant HairClub for Men, Ltd., Inc. is a Florida Corporation with its principal place of business at 1499 W. Palmetto Park Rd. Ste. 300 Boca Raton, FL, 33486-3311.

## **JURISDICTION & VENUE**

16. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of interest and costs. There are over 100 putative Class Members.

17. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in Florida, and regularly conducts business in Florida.

18. As Defendant operates more than 120 locations throughout the United States, Canada, and Puerto Rico, and Plaintiff seeks to certify a nationwide class, at least one unnamed class member is a non-Florida citizen<sup>3</sup> and resident and, thus, is diverse from Defendant, which is a Florida citizen.

19. Venue is proper in this Court because Defendant's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

## **FACTUAL ALLEGATIONS**

### ***HairClub for Men***

20. HairClub is a hair loss solution company that claims to be "North America's number one provider of hair regrowth, replacement, and restoration solutions."<sup>4</sup> It boasts a staggering annual revenue of \$53 million.<sup>5</sup>

21. As part of its business, Defendant receives, collects, and maintains the highly sensitive PII of its employees. In doing so, Defendant implicitly promises to safeguard their PII.

22. After collecting its employees' PII, Defendant maintains the PII in its computer

---

<sup>3</sup> In its Data Breach Notification to the Maine Attorney General, Defendant represented that one Maine resident was affected by the breach. *See* note 2.

<sup>4</sup> *HairClub Celebrates Season of Giving by Helping Seniors in Need*, HairClub, <https://www.hairclub.com/press-release/hairclub-celebrates-season-of-giving-by-helping-seniors-in-need-2/> (last visited March 20, 2024).

<sup>5</sup> HairClub Revenue, Zippia, <https://www.zippia.com/hair-club-careers-25508/revenue/> (last visited March 20, 2024).

systems. On information and belief, Defendant maintains former employees' PII for years after the employee-employer relationship is terminated.

23. In collecting and maintaining employees' PII, Defendant agreed it would safeguard the data in accordance with its internal policies as well as state law and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their PII.

24. Indeed, Defendant understood the importance of adequate cybersecurity measures, declaring in its Privacy Policy that "we respect your concerns about privacy and we take steps to protect it."<sup>6</sup>

25. Defendant further states that it is "committed to ensuring that the information you provide to us is used in accordance to the terms of this Policy and applicable law."<sup>7</sup>

26. Defendant understood the need to protect its employees' PII and prioritize its data security.

27. Despite recognizing its duty to do so, on information and belief, Defendant has not implemented reasonably cybersecurity safeguards or policies to protect employees' PII or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, Defendant leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to employees' PII.

### ***The Data Breach***

28. Plaintiff is a former employee of HairClub or its subsidiaries.

29. As a condition of employment with HairClub, employees were required to disclose their PII to Defendant and its subsidiaries, including but not limited to, their names, Social Security numbers, driver's license information, and financial account information. Defendant used that PII

---

<sup>6</sup> Privacy Policy, HairClub, <https://www.hairclub.com/privacy-policy/> (last visited March 20, 2024).

<sup>7</sup> *Id.*

to facilitate employment of Plaintiff, including payroll, and required Plaintiff to provide that PII to obtain employment and payment for that employment.

30. On information and belief, HairClub collects and maintains former and current employees' unencrypted PII in its computer systems.

31. In collecting and maintaining the PII, HairClub implicitly agrees it will safeguard the data using reasonable means according to its internal policies and federal law.

32. According to the Breach Notice, Defendant claims it "recently completed an investigation into an incident involving unauthorized access to certain systems on our network." Due to Defendant's obfuscating information, the precise dates on which the Data breach occurred and how long cybercriminals had access to Plaintiff's and the Class's most sensitive information is unclear. However, on information and belief, the breach took place between October 17, 2023 and October 18, 2023.<sup>8</sup>

33. Defendant's investigation "identified certain files and folders which may have been accessed without authorization." Upon completion of its investigation on December 1, 2023, Defendant revealed that the files involved in the breach included employees' "name, Social Security number, driver's license information, direct deposit account information and or medical information related to injuries at work or requests for family or medical leave." Ex. A.

34. In other words, the Data Breach investigation revealed HairClub's cyber and data security systems were completely inadequate and allowed cybercriminals to obtain files containing a treasure trove of its employees' highly private information.

35. Additionally, Defendant admitted that PII may have actually been stolen during the

---

<sup>8</sup> Data Breach Notifications, Office of the Maine Attorney General, <https://apps.web.maine.gov/online/aeviewer/ME/40/d570ad19-5ac8-4b21-8b2c-1330a5e7c386.shtml> (last visited March 20, 2024).

Data Breach confessing that the information was not just accessed, but “may have been taken” from HairClub’s system. Ex. A.

36. Through its inadequate security practices, Defendant exposed Plaintiff’s and the Class’s PII for theft and sale on the dark web.

37. On or about January 12, 2023 – over a month after Defendant completed its investigation – Defendant finally began notifying Plaintiff and Class Members about the Data Breach.

38. Despite its duties and alleged commitments to safeguard PII, Defendant did not in fact follow industry standard practices in securing employees’ PII, as evidenced by the Data Breach.

39. In response to the Data Breach, Defendant contends that it has “taken steps to further enhance our existing security measures.” Ex. A. Although Defendant does not elaborate on what these “steps” are, such enhancements should have been in place before the Data Breach.

40. On information and belief, Defendant has offered 12 months of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves PII that cannot be changed, such as Social Security numbers.

41. Even with several months of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff’s and Class Members’ PII is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

42. Cybercriminals need not harvest a person’s Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff’s and the Class’s PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other

sources to create “Fullz” packages, which can then be used to commit fraudulent account activity on Plaintiff’s and the Class’s financial accounts.

43. On information and belief, Defendant failed to adequately train and supervise its IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its employees’ PII. Defendant’s negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII.

***The Data Breach was a Foreseeable Risk of Which Defendant were on Notice.***

44. It is well known that PII, including Social Security numbers, is an invaluable commodity and a frequent target of hackers.

45. In 2021, there were a record 1,862 data breaches, surpassing both 2020’s total of 1,108 and the previous record of 1,506 set in 2017.<sup>9</sup>

46. In light of recent high profile data breaches, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), HairClub knew or should have known that its electronic records would be targeted by cybercriminals.

47. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

48. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of its duties to keep PII private and secure,

---

<sup>9</sup> Data breaches break record in 2021, CNET (Jan. 24, 2022), <https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/> (last visited March 20, 2024).

Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

49. In the years immediately preceding the Data Breach, Defendant knew or should have known that its computer systems were a target for cybersecurity attacks, including ransomware attacks involving data theft, because warnings were readily available and accessible via the internet.

50. In October 2019, the Federal Bureau of Investigation published online an article titled “High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations” that, among other things, warned that “[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector.”<sup>10</sup>

51. In April 2020, ZDNet reported, in an article titled “Ransomware mentioned in 1,000+ SEC filings over the past year,” that “[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay.”<sup>11</sup>

52. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a “Ransomware Guide” advising that “[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms

---

<sup>10</sup> October 02, 2019 Public Service Announcement, FBI, <https://www.ic3.gov/Media/Y2019/PSA191002> (last visited March 20, 2024).

<sup>11</sup> Ransomware Mentioned in 1,000+ SEC Filings Over the Past Year, ZDNET (April 30, 2020), <https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/> (last visited March 20, 2024).

of extortion.”<sup>12</sup>

53. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that (i) ransomware actors were targeting entities such as Defendant, (ii) ransomware gangs were ferociously aggressive in their pursuit of entities such as Defendant, (iii) ransomware gangs were leaking corporate information on dark web portals, and (iv) ransomware tactics included threatening to release stolen data.

54. In light of the information readily available and accessible on the internet before the Data Breach, Defendant, having elected to store the unencrypted PII of thousands of its employees in an Internet-accessible environment, had reason to be on guard for the exfiltration of the PII.

55. Before the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiff’s and Class Members’ PII could be accessed, exfiltrated, and published as the result of a cyberattack. Notably, data breaches are prevalent in today’s society therefore making the risk of experiencing a data breach entirely foreseeable to Defendant.

56. Prior to the Data Breach, Defendant knew or should have known that it should have encrypted its employees’ Social Security numbers and other sensitive data elements within the PII to protect against their publication and misuse in the event of a cyberattack.

### ***Plaintiff’s Experience and Injuries***

57. From approximately 2003 until 2018, Plaintiff Tittsworth was employed by HairClub.

58. As a condition of employment, HairClub required Plaintiff to provide her PII, including but not limited to her full name, address, Social Security number, and financial account

---

<sup>12</sup> Stop Ransomware Guide, CISA, <https://www.cisa.gov/stopransomware/ransomware-guide> (last visited March 20, 2024).

information.

59. Plaintiff provided her PII to HairClub and trusted that the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law.

60. Plaintiff Tittsworth received a Breach Notice on or around January 12, 2023, from Defendant, indicating that her PII, including at least her full name, driver's license information, Social Security number, medical information, and financial information, may have been compromised in the Data Breach. In addition to the damages detailed herein, the Data Breach has caused Plaintiff Tittsworth to be at substantial risk for further identity theft.

61. Defendant deprived Plaintiff of the earliest opportunity to guard herself against the Data Breach's effects by failing to notify her about it for over two months after the Data Breach occurred.

62. Plaintiff suffered actual injury from the exposure of her PII—which violates her rights to privacy.

63. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

64. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's PII for theft by cybercriminals and sale on the dark web.

65. Defendant also deprived Plaintiff of the earliest opportunity to guard herself against the Data Breach's effects by failing to notify her about it in a timely manner.

66. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice

of Data Breach and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

67. Plaintiff has and will spend considerable time and effort monitoring her accounts to protect herself from additional identity theft. Plaintiff fears for her personal financial security and uncertainty over what PII was exposed in the Data Breach.

68. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

69. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

70. Plaintiff has an imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties and possibly criminals.

71. Indeed, following the Data Breach, Plaintiff began experiencing spam texts, phone calls, and emails, suggesting that her PII has been placed in the hands of cybercriminals.

72. Plaintiff has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

***Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft***

73. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

74. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and the

proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. Plaintiff and the Class have suffered or are at an increased risk of suffering:

- a. The loss of the opportunity to control how their PII is used;
- b. The diminution in value of their PII;
- c. The compromise and continuing publication of their PII;
- d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;
- e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;
- f. Delay in receipt of tax refund monies;
- g. Unauthorized use of stolen PII; and
- h. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in its possession.

75. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to \$1,000.00 depending on the type of information obtained.

76. The value of Plaintiff's and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen

private information openly and directly on various “dark web” internet websites, making the information publicly available, for a substantial fee of course.

77. Social Security numbers are particularly attractive targets for hackers because they can easily be used to perpetrate identity theft and other highly profitable types of fraud. Moreover, Social Security numbers are difficult to replace, as victims are unable to obtain a new number until the damage is done.

78. It can take victims years to spot identity or PII theft, giving criminals plenty of time to use that information for cash.

79. One such example of criminals using PII for profit is the development of “Fullz” packages.

80. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as “Fullz” packages.

81. The development of “Fullz” packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff’s and the Class’s phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and the Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff’s and members of the Class’s stolen PII is being misused, and that such misuse is fairly traceable to the Data

Breach.

82. Defendant disclosed the PII of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII. Defendant's failure to properly notify Plaintiff and the Class of the Data Breach exacerbated Plaintiff's and the Class's injuries by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

***Defendant failed to adhere to FTC guidelines.***

83. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

84. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

- a. protect the personal customer information that they keep;
- b. properly dispose of personal information that is no longer needed;
- c. encrypt information stored on computer networks;
- d. understand its network's vulnerabilities; and
- e. implement policies to correct security problems.

85. The guidelines also recommend that businesses watch for large amounts of data

being transmitted from the system and have a response plan ready in the event of a breach.

86. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

87. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer, data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet its data security obligations.

88. Defendant’s failure to employ reasonable and appropriate measures to protect against unauthorized access to employees’ PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

***Defendant Failed to Follow Industry Standards***

89. Several best practices have been identified that—at a minimum—should be implemented by businesses like Defendant. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

90. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email

management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

91. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

92. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

### **CLASS ACTION ALLEGATIONS**

93. Plaintiff sues on behalf of herself and the proposed nationwide class ("Class"), defined as follows, pursuant to Federal Rule of Civil Procedure 23(b)(2) and (b)(3):

**All individuals residing in the United States whose PII was compromised in the Data Breach, including all those who received notice of the breach.**

94. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any of Defendant's officers or directors, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

95. Plaintiff reserves the right to amend the class definition.

96. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity.** The members of the Class are so numerous that joinder of all members of the Class is impracticable. Plaintiff is informed and believes that the proposed Class includes a staggering 4334 individuals who have been damaged by Defendant's conduct as alleged herein.

b. **Ascertainability.** Members of the Class are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality.** Plaintiff's claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy.** Plaintiff will fairly and adequately protect the proposed Class's interests. Her interests do not conflict with the Class's interests, and she has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality.** Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

- i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII;
- ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- iii. Whether Defendant was negligent in maintaining, protecting, and securing PII;

- iv. Whether Defendant breached contract promises to safeguard Plaintiff's and the Class's PII;
- v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;
- vi. Whether Defendant's Breach Notice was reasonable;
- vii. Whether the Data Breach caused Plaintiff's and the Class's injuries;
- viii. What the proper damages measure is; and
- ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

97. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

**COUNT I**  
**Negligence**  
**(Against Defendant On Behalf of Plaintiff and the Class)**

98. Plaintiff and members of the Class incorporate the allegations in paragraphs 1–97 as if fully set forth herein.

99. Defendant owed to Plaintiff and the Class a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

100. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII—

just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and members of the Class's PII by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

101. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and members of the Class to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

102. Defendant owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and the Class's personal information and PII.

103. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII—whether by malware or otherwise.

104. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and members of the Class and the importance of exercising reasonable care in handling it.

105. Defendant breached its duties by failing to exercise reasonable care in handling and securing the personal information and PII of Plaintiff and members of the Class which actually and proximately caused the Data Breach and Plaintiff's and members of the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and members of the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

106. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

**Count II**  
**Negligence *Per Se***  
**(Against Defendant On Behalf of Plaintiff and the Class)**

107. Plaintiff and members of the Class incorporate the allegations in paragraphs 1–97 as if fully set forth herein.

108. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant has a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and members of the Class's PII.

109. Section 5 of the FTC Act prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect employees’ PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant’s duty to protect Plaintiff’s and the Class’s sensitive PII.

110. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards as described in detail herein. Defendant’s conduct was particularly unreasonable given the nature and amount of PII Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

111. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

112. Defendant has a duty to Plaintiff and the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiff’s and the Class’s PII.

113. Defendant breached its duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff’s and members of the Class’s PII.

114. Defendant’s violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

115. But for Defendant’s wrongful and negligent breach of its duties owed to Plaintiff

and members of the Class, Plaintiff and the Class would not have been injured.

116. The injury and harm suffered by Plaintiff and the Class were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

117. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

**Count III**  
**Breach of Fiduciary Duty**  
**(Against Defendant On Behalf of Plaintiff and the Class)**

118. Plaintiff and members of the Class incorporate the allegations in paragraphs 1–97 as if fully set forth herein.

119. Given the relationship between Defendant and Plaintiff and Class Members, where Defendant became guardian of Plaintiff's and Class Members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' PII; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

120. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant's relationship with them—especially to secure their PII.

121. Because of the highly sensitive nature of the PII, Plaintiff and Class Members would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII had they known the reality of Defendant's inadequate data security practices.

122. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class Members' PII.

123. Defendant also breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

124. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

**Count IV**  
**Breach of Implied Contract**  
**(Against Defendant On Behalf of Plaintiff and the Class)**

125. Plaintiff and members of the Class incorporate the allegations in paragraphs 1–97 as if fully set forth herein.

126. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of receiving employment from Defendant. Plaintiff and Class Members provided their PII to Defendant in exchange for Defendant's employment.

127. Plaintiff and Class Members reasonably understood that a portion of the funds from their employment would be by Defendant used to pay for adequate cybersecurity and protection of their PII.

128. Plaintiff and the Class Members accepted Defendant's offers by disclosing their PII to Defendant in exchange for employment.

129. Plaintiff and Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members if and when their data had been breached and compromised. Each such contractual relationship imposed on Defendant an implied covenant of good faith and fair dealing by which Defendant was required to perform its obligations and manage Plaintiff's and Class Members' data in a manner which comported with the reasonable expectations of privacy and protection attendant to entrusting such data to Defendant.

130. In providing their PII, Plaintiff and Class Members entered into an implied contract with Defendant whereby Defendant, in receiving such data, became obligated to reasonably safeguard Plaintiff's and the other Class Members' PII.

131. In delivering their PII to Defendant, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard that data.

132. Plaintiff and the Class Members would not have entrusted their PII to Defendant in the absence of such an implied contract.

133. Defendant accepted possession of Plaintiff's and Class Members' PII.

134. Had Defendant disclosed to Plaintiff and Class Members that Defendant did not have adequate computer systems and security practices to secure employees' PII, Plaintiff and members of the Class would not have provided their PII to Defendant.

135. Defendant recognized that employees' PII is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and Class Members.

136. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

137. Defendant breached the implied contract with Plaintiff and Class Members by failing to take reasonable measures to safeguard their data.

138. Defendant breached the implied contract with Plaintiff and Class Members by failing to promptly notify them of the access to and exfiltration of their PII.

139. As a direct and proximate result of the breach of the contractual duties, Plaintiff and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiff and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and Class Members' PII; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their PII; (g) the diminution in the value of the services bargained for as Plaintiff and Class Members were deprived of the data protection and security that Defendant promised when Plaintiff and the proposed class entrusted Defendant with their PII; and (h) the continued and substantial risk to Plaintiff's and Class Members' PII, which remains in the Defendant's possession with inadequate measures to protect Plaintiff's and Class Members' PII.

**Count V**  
**Unjust Enrichment**  
**(Against Defendant On Behalf of Plaintiff and the Class)**

140. Plaintiff and members of the Class incorporate the allegations in paragraphs 1–97 as if fully set forth herein.

141. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

142. Plaintiff and Class Members conferred a monetary benefit on Defendant, by

providing Defendant with their valuable PII.

143. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII.

144. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and the Class, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

145. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

146. Defendant acquired the monetary benefit and PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

147. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

148. Plaintiff and Class Members have no adequate remedy at law.

149. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity how their PII is used; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future

consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

150. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm.

151. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

### **PRAYER FOR RELIEF**

Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

- A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing her counsel to represent the Class;
- B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;
- C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;
- D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

- E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;
- F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;
- G. Awarding attorneys' fees and costs, as allowed by law;
- H. Awarding prejudgment and post-judgment interest, as provided by law;
- I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and
- J. Granting such other or further relief as may be appropriate under the circumstances.

**JURY DEMAND**

Plaintiff hereby demands that this matter be tried before a jury.

Dated: March 20, 2024,

Respectfully Submitted,

/s/ Joshua R. Jacobson

Joshua R. Jacobson  
Florida Bar No. 1002264  
**JACOBSON PHILLIPS PLLC**  
478 E. Altamonte Dr., Ste. 108-570  
Altamonte Springs, FL 32701  
Telephone: (407) 720-4057  
joshua@jacobsonphillips.com

Raina Borrelli\*  
raina@turkestrauss.com  
**TURKE & STRAUSS LLP**  
613 Williamson Street, Suite 201  
Madison, Wisconsin 53703  
T: (608) 237-1775  
F: (608) 509-4423

*\* Pro hac vice forthcoming*

*Attorneys for Plaintiff and Proposed  
Class*